MA3H1 Topics in Number Theory
Example Sheet 4

You should attempt all the questions on this sheet, but questions Q2(i),Q3,Q5(i) will marked for credit, and must be handed in by **3pm Friday, week 7**.

(1) List (and memorise!) the squares modulo 4, 8, 3, 5, 7.

(2) (i) Show that the sequence $n^5 - n + 3$ does not contain any squares. **(Hint: consider modulo 5.)**
  (ii) Let p be a prime $p \equiv 3, 5 \pmod 8$. Show that the sequence $n! + n^p - n + 2$ contains at most finitely many squares.

(3) (i) Is 219 a square modulo 383?
  (ii) Is 219 a square modulo 143? (Be careful!)

(4) For which primes is 5 a quadratic residue? For which primes is 3 a quadratic residue?

(5) Suppose p, q are primes with $p = 2q + 1$.
  (i) Show that if $q \equiv 1 \pmod 4$ then 2 is a primitive root modulo p.
  (ii) Under what conditions on q is 5 a primitive root modulo p?

(6) Show that the equation $y^2 = x^3 + 7$ has no integral solutions. **(Hint: rewrite as $y^2 + 1 = x^3 + 8$.)**

(7) Let m be a positive odd integer. In this exercise we prove the identity

$$\frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{t=1}^{(m-1)/2} \left(\sin^2 x - \sin^2 \frac{2\pi t}{m} \right).$$

  (a) By induction on m (odd) show (simultaneously) that

$$\frac{\sin mx}{\sin x} = f_m(\sin^2 x), \qquad \frac{\cos mx}{\cos x} = g_m(\sin^2 x),$$

  where f_m and g_m are polynomials of degree $(m-1)/2$ with leading coefficient $(-4)^{(m-1)/2}$.
  (b) Show that $\sin^2 \frac{2\pi t}{m}$ with $t = 1, 2, \ldots, (m-1)/2$ are distinct roots of f_m.
  (c) Deduce the identity.